UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/484,691	01/18/2000	Hashem Mohammad Ebrahimi	1565.035US1	9980

21186 7590 10/27/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
10/27/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HASHEM MOHAMMAD EBRAHIMI
and ROBERT DREW MAJOR

Appeal 2009-002157
Application 09/484,691
Technology Center 2400

Decided: October 23, 2009

Before JOSEPH L. DIXON, LANCE LEONARD BARRY, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-31, which are all of the claims pending in this application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Invention

Appellants' invention relates to methods, signals, devices, and systems for using proxy servers to transparently forward messages between clients and origin servers if, and only if, doing so does not violate network policies. Abstract.

Representative Claim

1. A method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server, wherein the transparent proxy is unknown to the client;

redirecting the client request from the transparent proxy to a policy module;

obtaining at the transparent proxy policy enforcement data, wherein the policy enforcement data is received from the policy module and wherein the policy module and the transparent proxy reside within a same environment;

generating at the transparent proxy a policy state token in response to the policy enforcement data; and transmitting the policy state token from the transparent proxy to the client, wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy.

Prior Art

Birrell	5,805,803	Sep. 8, 1998
Green	6,003,084	Dec. 14, 1999
Makarios	6,401,125 B1	Jun. 4, 2002
Lim	6,728,884 B1	Apr. 27, 2004
Callaghan	2002/0007317 A1	Jan. 17, 2002

Examiner's Rejections

Claims 1-3, 7, 8, 9-17, and 20-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Makarios and Green.

Claims 4, 6, 18, 19, 29, and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, and Callaghan.

Claim 5 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, Callaghan, and Birrell.

Claim 31 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, and Lim.

Claim Groupings

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal on the basis of claim 1. *See* 37 C.F.R. § 41.37(c)(1)(vii).

ISSUE

Have Appellants shown that the Examiner erred in finding that Makarios teaches a transparent proxy?

FINDINGS OF FACT

Green

1. Green discloses a secure network proxy for connecting entities. Title.

2. A proxy which is part of a firewall program controls exchanges of information between two application entities. The proxy interrogates attempts to establish a communication session by requesting entities with a server entity in accordance with defined authentication procedures. The requestor's address and the server's address are checked against an access control list. If either address is invalid, the proxy closes the connection. If both are valid, a new connection is setup such that both the requestor and server are transparently connected to the proxy. Abstract.

3. The proxy is "transparent" because neither the requestor nor the client is aware of the proxy. The proxy performs a firewall function in support of a security policy. Col. 4, ll. 38-47.

4. In one embodiment, the proxy transparently receives and forwards transport packets in accordance with a defined security policy. Col. 5, ll. 25-27.

5. The proxy includes a connection manager portion and a security manager portion. Col. 5, ll. 35-37.

6. The security policy is implemented in the security manager portion substantially independently from the connection manager portion. Col. 6, ll. 5-7.

7. The security manager monitors data for conformance with predefined conditions and provides control information to the connection manager. The connection manager controls the proxy on whether to

establish connections to a server. These components, which are shown in Figure 3b, can interrogate all inbound requests for new sessions to ensure conformance to configured authentication procedures and authenticate the signature and certificates provided. Fig. 3b; col. 8, ll. 14-24; col. 9, ll. 25-34.

8. The requester's IP address (source) and the server's IP address (destination) are checked against an access control list (ACL). If either address is invalid the proxy closes the connection. If both addresses are valid the proxy attempts to set up a new connection with the server on the destination network. The requester is totally unaware this independent connection is taking place. Col. 10, ll. 8-27.

Makarios

9. Makarios discloses a system and method for maintaining state information between a web proxy server and its clients. Title.

10. A proxy can establish and maintain state information with a particular web client to, for example, maintain the identity of a user who is making a sequence of web requests to arbitrary servers located anywhere on the web via the proxy. Col. 2, ll. 54-60.

11. A distributed network communication system implements a series of token exchange transactions similar to those used when passing browser cookies between an Internet server and a browser client. A proxy cookie is stored on the client side at the behest of the web proxy. When the browser client presents a request for information to the proxy which is to be passed on to the Internet server, the proxy uses the proxy cookie to identify the originator of the request. Based on this, the proxy can customize and

personalize the client's information request as appropriate and pass the request on to the Internet server. Abstract.

12. The proxy is one component of a firewall, which protects an organization from outside threats and the release of information. The basic function of the proxy is to forward user requests for web documents to their ultimate destinations at various servers on the web and to relay responses back to users. This enables central administration of a single point of transmission through an organization's firewall. Col. 1, ll. 42-54.

13. The proxy monitors a request generated by the browser client for HTTP objects. The request is intercepted by the proxy to see if the request contains a cookie, which is used as an index for personalizing the client's information request. For example, a user ID specified in the cookie may be used to index a table of attributes used in personalization operations for that particular user. Col. 4, ll. 30-48.

14. If no proxy cookie was included in the request from the client, the proxy redirects the client to a new web page. The user enters information into the web page and the proxy directs the client to store a proxy cookie. Col. 4, l. 49 to col. 5, l. 30.

Appellants' Specification

15. Figure 4 illustrates conventional use of a transparent proxy 400. Unlike the known proxy servers 200 and 300, the transparent proxy server 400 is unknown to the user agent 100. That is, the user agent 100 itself has not been configured to communicate with the transparent proxy 400. Instead, the transparent proxy 400 is inserted in the communication path by means of capturing network traffic at a router or gateway with access to all

traffic transmitted between the user agent 100 and the origin server 102. This capture is effected without any modification to the user agent 100. The transparent proxy 400 may be inserted to perform caching or to enforce access control policy on user agent requests. Fig. 4; Spec. 6:11-18.

16. "Transparent" does not mean "undetectable," for the presence of transparent proxy may be detected by noting the redirection during step 702 (Fig. 7), for instance. Rather, "transparent" means that the effects of the proxy on the client are limited to policy enforcement. Spec. 26:20 to 27:1.

17. Figure 2 illustrates conventional tools and techniques for using a known proxy server 200 to filter out cookies. The proxy server 200 is known to the user agent 100 in the sense that the IP address, domain name, or other identifying information about the proxy server 200 has been stored on the user agent 100 to configure the user agent 100 so that the user agent 100 expressly directs a request 202 to the proxy server 200 for origin server 102 resources. For instance, commonly used web browsers allow one to specify a proxy server by entering the server's IP address through the application's configuration user interface. Spec. 4:8-14.

18. In general, a state token is a data structure that contains state data that helps define a contextual relationship between particular computer processes. For instance, "cookies" used to define the context of a relationship between a client and an origin server are state tokens. Spec. 23:10-13.

PRINCIPLES OF LAW

Claim Interpretation

During examination, claims are to be given their broadest reasonable interpretation consistent with the specification, and the language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Amer. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations omitted). The Office must apply the broadest reasonable meaning to the claim language, taking into account any definitions presented in the specification. *Id.* (citing *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002)).

Obviousness

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007).

ANALYSIS

The Examiner finds that Makarios discloses a transparent proxy that performs policy enforcement for a client (Ans. 3-4). Appellants contend that Makarios "teaches away" from a transparent proxy, because the client is aware of the proxy and must register with the proxy (App. Br. 11-12). However, Appellants have not provided a definition of the term "transparent

proxy" that excludes a client from being aware of a proxy or from providing information to a proxy. For example, Appellants' Specification states that "transparent" does not mean "undetectable," for the presence of a transparent proxy may be detected. Rather, "transparent" means that the effects of the proxy on the client are limited to policy enforcement. FF 16. Appellants contrast a transparent proxy with what Appellants call a "known proxy," which is known in the sense that the IP address, domain name, or other identifying information about the proxy server has been stored on the user agent to configure the user agent so that the user agent expressly directs a request to the proxy server for origin server resources. FF 17.

Appellants have not provided any evidence to show that the effects of the proxy on the client as described in Makarios are not "limited to policy enforcement." Appellants have also not provided any evidence to show that, in Makarios, the "IP address, domain name, or other identifying information about the proxy server . . . has been stored on the user agent . . . to configure the user agent . . . so that the user agent . . . expressly directs a request . . . to the proxy server . . . for origin server . . . resources." Appellants have therefore failed to persuasively rebut the Examiner's finding that Makarios discloses a transparent proxy that performs policy enforcement for a client.

Appellants' arguments that Makarios and Green "teach away" from one another (App. Br. 12); that Makarios would be inoperable if it included a transparent proxy (App. Br. 12-13); and that adding a transparent proxy to Makarios would make it inoperable (App. Br. 13), are based on the premise that Makarios does not disclose a transparent proxy. However, Appellants have failed to establish this allegation as fact. Therefore, we find these arguments unpersuasive.

Appellants contend that the Examiner performed improper hindsight in combining Makarios with Green because the teachings of Makarios rely on a forward proxy and Green relies on a transparent proxy (App. Br. 13-14). The Examiner finds that adding the security features of Green to the proxy of Makarios provides several benefits, including more security and more versatility (Ans. 5). Appellants fail to address this motivation described by the Examiner; rather, Appellants rely on the premise that Makarios does not disclose a transparent proxy as support for their improper hindsight contention. Because Makarios discloses a transparent proxy within the meaning of claim 1, we find Appellants' improper hindsight argument unpersuasive.

Appellants present a new argument in the Reply Brief contending that Makarios and Green, even if combined, do not teach authentication of a client to a transparent proxy (Reply Br. 3). Appellants also raise new arguments contending that one of ordinary skill in the art would not combine a reference addressing customized presentation of information with a reference addressing a method of authenticating a client and a server, and that the combination does not teach a policy module residing within an environment of the proxy (Reply Br. 4).

The purpose of a reply brief is to provide an appellant the opportunity to have the last word. The reply brief enables the appellant to address any new grounds of rejection the Examiner may have raised in the answer, or to address changes or developments in the law that may have occurred after the principal brief was filed. The reply brief is *not* an opportunity to make arguments that could have been made during prosecution, but were not. Nor is the reply brief an opportunity to make arguments to rebut the Examiner's

rejections that could have been made in the principal brief on appeal, but were not. The Rules do not require the Board to take up a belated argument that has not been addressed by the Examiner, absent a showing of good cause.

Even so, in response to Appellants' new arguments that the combination of Makarios and Green does not teach authentication of a client to a transparent proxy, does not teach that the policy module is in the environment of the proxy, and that one of ordinary skill in the art would not combine the teachings of Makarios and Green, we find the following.

Green discloses a proxy in a firewall that receives a request from a client requesting a resource of an origin server (FF 1-2). The transparent proxy is unknown to the client (FF 3). The client request is redirected to a security policy module (FF 4-8). Authentication and security policy enforcement data is obtained at the transparent proxy, wherein the security policy enforcement data is received from the security policy module (*id.*). The security policy module and the transparent proxy reside in the same environment (*id.*).

Makarios discloses a proxy in a firewall that monitors client requests for HTTP objects (FF 12-13). If the request does not contain a proxy cookie, the client is redirected to a new web page and directs the client to store a proxy cookie (FF 14). The proxy cookie is used to establish and maintain state information with a particular web client to maintain the identity of a user who is making a sequence of web requests to servers via the proxy (FF 9-11).

A person of ordinary skill in the art at the time of invention, after obtaining authentication and policy enforcement data for a client at a proxy

as disclosed by Green (FF 1-8), would have generated and transmitted a state token cookie from the proxy to the client as disclosed by Makarios (FF 9-14) for the benefit of maintaining the authentication and security policy state information of the client for subsequent interactions between the client and the proxy as taught by Makarios (FF 9-11).

CONCLUSION OF LAW

Appellants have failed to show that the Examiner erred in finding that Makarios teaches a transparent proxy.

DECISION

The rejection of claims 1-3, 7, 8, 9-17, and 20-28 under 35 U.S.C. § 103(a) as being unpatentable over Makarios and Green is affirmed.

The rejection of claims 4, 6, 18, 19, 29, and 30 under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, and Callaghan is affirmed.

The rejection of claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, Callaghan, and Birrell is affirmed.

The rejection of claim 31 under 35 U.S.C. § 103(a) as being unpatentable over Makarios, Green, and Lim is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED

msc

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS MN 55402